HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200207237-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Christoph Gouguenheim et al.

Confirmation No.: 2133

Application No.: 10/733,434

Examiner: Laurel L. Lashley

Filing Date: December 10, 2003

Group Art Unit: 2132

Title: TRUSTED SYSTEM FOR FILE DISTRIBUTION

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on March 11, 2008.

☒ The fee for filing this Appeal Brief is $510.00 (37 CFR 41.20).

☐ No Additional Fee Required.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $460	☐ 3rd Month $1050	☐ 4th Month $1640

☐ The extension fee has already been filed in this application.

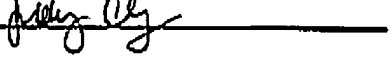
☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

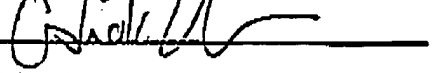
Please charge to Deposit Account 08-2025 the sum of $ 510. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☐ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit:

OR

☒ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile: May 12, 2008
Typed Name: Judy H. Chung
Signature: 

Respectfully submitted,
Christoph Gouguenheim et al.
By 
Ashok K. Mannava
Attorney/Agent for Applicant(s)
Reg No.: 45,301
Date: May 12, 2008
Telephone: (703) 652-3822

Rev 10/07(ApiBrief)

Total number of pages: 25

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 200207237-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Christoph Gouguenheim et al.	**Confirmation No.:**	2133
Serial No.:	10/733,434	**Examiner:**	Laurel L. Lashley
Filed:	December 10, 2003	**Group Art Unit:**	2132
Title:	TRUSTED SYSTEM FOR FILE DISTRIBUTION		

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a Final Office Action, including final rejection, dated December 19, 2007, and the Notice of Appeal filed on March 11, 2008. It is respectfully submitted that the present application has been more than twice rejected. Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith and labeled appropriately.

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

TABLE OF CONTENTS

RECEIVED
CENTRAL FAX CENTER

MAY 12 2008

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

(1) Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The Appellant is unaware of any appeals or interferences related to this case.

(3) Status of Claims

Claims 1-28 and 30-36 are pending in the present application of which claims 1, 11, 17, 19, 26, 28 and 36 are independent.

Claim 29 is canceled.

Claims 1-28 and 30-36 are rejected.

Claims 1-28 and 30-36 are appealed.

(4) Status of Amendments

No amendment was filed subsequent to the Final Office Action dated December 19, 2007.

(5) Summary of Claimed Subject Matter

It should be understood that the subject matter of the independent claims and dependent claims recited below is supported in at least the following cited sections of the present

application. Thus, other sections in the present application may provide the same or additional supports as well.

Independent Claims

Claim 1. A secure token for use with an encrypted file and an insecure decryption device, the secure token comprising a processor for protecting a first cryptographic key against unauthorized access, and (paragraphs 22 and 25, fig 2) creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device. (paragraph 32, fig 3)

Claim 11. An article for a secure device, the secure device including a processor, the secure device used in combination with an insecure device, (paragraphs 22 and 25, fig 2) the article comprising memory encoded with data for instructing the processor to protect a first cryptographic key against unauthorized access (paragraph 31), use a hash function to create a second cryptographic key from the first key and a message unique to the insecure device, and send the second key to the insecure device. (paragraph 35, fig 4)

Claim 17. A data rights management server for use with a media transaction system, (fig 1) the server comprising a processing unit programmed to cause the server to establish a secure channel with a smart card, access a unique identifier corresponding to an insecure device, (paragraph 29, fig 3) send a first cryptographic key to the smart card via the secure channel, (paragraph 29, fig

3) receive a unique identifier from the insecure device, create a second key from the first key and the identifier (paragraphs 32-33, fig 3); encrypt a media file with the second key, and send the encrypted media file to the insecure device, the first key corresponding to the media file. (paragraphs 32-34, fig 3)

Claim 19. A method of using an insecure decryption device for file distribution, the method comprising:

accessing a message unique to the insecure device; (paragraphs 60-61, fig 7)

accessing a first cryptographic key; (paragraphs 60-61, fig 7)

creating a second cryptographic key from the message and the first key; and (paragraphs 63-64, fig 7)

allowing the insecure device to access the second key but not the first key; whereby the insecure device can use the second key for decryption. (paragraph 65, fig 7)

Claim 26. An insecure decryption device for use with a secure device and a first cryptographic key, the device comprising: (fig 1)

means for sending a message to the secure device, the message unique to the insecure device; (paragraphs 60-61, fig 7 and paragraph 27, figs 3-4)

means for receiving a second cryptographic key from the secure device, the second cryptographic key derived from the message and the first cryptographic key; and (paragraphs 65-66, fig 7 and paragraph 32-34, figs 3-4)

means for performing decryption with the second cryptographic key. (paragraph 66, fig 7 and paragraph 35, figs 3-4)

Claim 28. A trusted system for file distribution, the system comprising:

an insecure device; (figs 1 and 6) and

a trusted secure device for storing a first cryptographic key, accessing a message from the insecure device wherein the message is unique to the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting file access rights; (figs 3 and 7, paragraphs 27-34 and 59-69)

the insecure device not allowed to access the first key, the insecure device using the second key for decryption. (figs 3 and 7, paragraphs 27-34 and 59-69)

Claim 36. A trusted media transaction system comprising

an insecure media player; and (figs 1 and 6)

a trusted secure token for performing an electronic transaction to obtain a first cryptographic key, accessing a message from the insecure device wherein the message is unique to the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting media file access rights; (figs 3 and 7, paragraphs 27-34 and 59-69)

the insecure device configured to use the second key for media file decryption. (figs 3 and 7, paragraphs 27-34 and 59-69)

Dependent Claims

Claim 7. The secure token of claim 4, wherein the secure token conducts a transaction with a peer to sell a file; and wherein the secure token sends the first key to the peer. (paragraphs 21, 22, 27-32, 36-43)

Claim 8. The secure token of claim 7, wherein the secure token creates a third key that is unique to the peer, and sends the third key to the insecure device and the peer. (paragraphs 21, 22, 27-32, 36-43)

Claim 15. The article of claim 13, wherein the secure device conducts a transaction with a peer to sell a file; and wherein the secure device sends the first key to the peer. (paragraphs 21, 22, 27-32, 36-43)

Claim 16. The article of claim 15, wherein the data further instructs the processor to create a third key that is unique to the peer, sends the third key to the insecure device and the peer. (paragraphs 21, 22, 27-32, 36-43)

Claim 24. The method of claim 21, wherein the electronic transaction is conducted with a peer to sell a file; the method further comprising sending the first key to the peer. (paragraphs 21, 22, 27-32, 36-43)

Claim 25. The method of claim 24, further comprising creating a third key that is unique to the peer, and sending the third key to the insecure device and the peer. (paragraphs 21, 22, 27-32, 36-43)

(6) Grounds of Rejection to be Reviewed on Appeal

A. Claims 1-36 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

B. Claims 1-28 and 30-36 are rejected under 35 U.S.C. §102(b) as being anticipated by Kocher et al. (6,289,455), referred to as Kocher.

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

(7) Arguments

A. The rejection of claims 1-36 under 112 2nd paragraph should be reversed because claims 1-28 and 30-36 are definite.

Claims 1-36 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Note that claim 29 was previously canceled, so the rejection incorrectly rejects claim 29.

Independent claim 1 was rejected because "the first key", "the second key", and "the insecure device" allegedly lack antecedent basis. Independent claim 1 and its dependent claims only reference one first key (*i.e.*, a first cryptographic key), and only reference one second key (*i.e.*, a second cryptographic key), and only reference one insecure device (*i.e.*, an insecure decryption device). Accordingly, the Applicants believe "the first key" clearly refers to the claimed first cryptographic key, "the second key" clearly refers to the claimed second cryptographic key, and "the insecure device" clearly refers to the claimed insecure decryption device. Thus claim 1 is believed to be definite. Similar rejections were made for independent claims 11, 17, 19, 26, 28 and 36, and these claims are also believed to be definite.

For at least these reasons, the rejections under 112 second paragraph should be reversed.

B. The rejection of claims 1-28 and 30-36 under 35 U.S.C. §102(b) as being anticipated by Kocher should be reversed because Kocher fails to teach all the claimed features.

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

Claims 1-36 were rejected under 35 U.S.C. §102(b) as being anticipated by Kocher.

According to an embodiment described in the Applicants' specification, a device, such as a media player, that is operable to read a secure token, sends its unique ID, N_j, to a server, for example, to purchase a media file. After the purchase, the server sends a first cryptographic key K_1 to the secure token. The server also uses a secure hash function to generate a second cryptographic key K_2 from the first cryptographic key and the unique ID of the media player as follows: $K_2=H(K_1,N_j)$. The server encrypts the media file with K_2 and sends it to the media

player. The secure token gets N_j from the media player and calculates K_2, and sends K_2 to the media player. The media player may then decrypt the media file with K_2 received from the secure token and play the media file. See paragraphs 27-34 and figure 3. The unique ID of the device is a message of the device, such as a serial number. Another type of message unique to the media player and stored in the media player may be used to generate K_2. See paragraph 62. As described above, it should be noted that in these embodiments, a message unique to the media player, such as serial number, is used to generate K_2.

Claim 1 recites,

> creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device.

Kocher fails to teach creating a second key from a first key and a message unique to an insecure device. The rejection alleges this feature is taught in col. 8, lines 17-28 of Kocher. In this passage, Kocher discloses a Key Derivation Message (KDM), which is a message generated by the content provider to allow a CRU to derive a key corresponding to digital content, and the KDM is usually transmitted with the content.

However, Kocher fails to teach that the KDM is unique to an insecure device. Instead, unlike the embodiments of the Applicants' invention where the unique message is initially stored in the insecure device and sent to the server, in Kocher the KDM is generated by the content provider and sent to the playback device 210. Thus, it appears Kocher generates a KDM for each content rather than a KDM unique to the playback device. There is clearly no disclosure

and no other support, either expressly or inherently, in Kocher teaching the KDM is unique to the playback device 210.

In the Response to Arguments section in the Final Office Action, page 3, the Examiner states that since digital content is variable, the message (referring to the KDM) is unique to the device. As described above, this assumption is not supported by the disclosure of Kocher. Instead, the KDM clearly could be unique to the content. Thus, the content could be played on different devices.

Independent claim 11 recites using a hash function to create a second key from the first key and a message unique to the insecure device. Kocher fails to teach the message unique to the insecure device, or using a hash function to create a second key from the first key and the message unique to the insecure device.

Regarding these features of claim 11, for the reasons set forth above with respect to claim 1, Kocher fails to teach the message unique to the insecure device. Regarding the hash function, Kocher discloses a pseudoasymmetric function in column 8, lines 28-44. Lines 39-44 disclose that the function is used for encryption. Claim 11 recites using a hash function to create a second key from the first key and the message unique to the insecure device. Claim 11 does not reciting using the hash function to encrypt. Kocher fails to teach using a hash function to create a second key.

Independent claim 17 recites a data rights management server receiving a unique identifier from the insecure device. As described above, Kocher fails to teach the content provider receiving a unique identifier for the playback device from the playback device. Instead,

the KDM is generated at the content provider and is not received from the playback device. Also, Kocher fails to teach the KDM is unique to the playback device.

Independent claims 19, 28 and 36 recite accessing a message unique to the insecure device. Independent claim 26 recites sending a message unique to the insecure device. These features are not taught by Kocher for the reasons stated above.

Many of the features of the dependent claims are not taught by Kocher.

Claim 7 recites the secure token conducts a transaction with a peer to sell a file.

Claim 8 recites the secure token creates a third key unique the peer and sends the third key to the peer and the insecure device. Kocher fails to teach the smart card is used to sell a file, and fails to teach creating a third key for the peer and sending the third key to both the peer and the playback device.

Claim 15, 16, 24 and 25 recite similar features.

None of these features of claims 7, 8, 15, 16, 24 and 25 are taught by Kocher.

For at least these reasons claims 1-28 and 30-36 are believed to be allowable.

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

(8) Conclusion

For at least the reasons given above, the rejection of claims 1-43 described above and the objection to the Abstract described above should be reversed and these claims allowed.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

Respectfully submitted,

Dated: May 12, 2008 By

Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
11240 Waples Mill Road
Suite 300
Fairfax, VA 22030
(703) 652-3822
(703) 865-5150 (facsimile)

(9) Claim Appendix

1. A secure token for use with an encrypted file and an insecure decryption device, the secure token comprising a processor for protecting a first cryptographic key against unauthorized access, and creating a second cryptographic key from the first key and a message unique to the insecure device, the second key usable for file decryption by the insecure device.

2. The secure token of claim 1 wherein the secure token includes a smart card, the smart card including the processor.

3. The secure token of claim 1, wherein the processor uses a hash function to create the second key from the message and the first key.

4. The secure token of claim 1, wherein the secure token performs an electronic transaction to obtain the first key.

5. The secure token of claim 4, wherein the secure token conducts a transaction with a server to purchase a desired file; and wherein the secure token receives the first key from the server.

6. The secure token of claim 4, wherein the secure token conducts a transaction with a peer to purchase a file; and wherein the secure token receives the first key from the peer.

7. The secure token of claim 4, wherein the secure token conducts a transaction with a peer to sell a file; and wherein the secure token sends the first key to the peer.

8. The secure token of claim 7, wherein the secure token creates a third key that is unique to the peer, and sends the third key to the insecure device and the peer.

9. The secure token of claim 1, further comprising means for receiving the first key and encrypted data, wherein the insecure device uses the second key to decrypt the encrypted data.

10. The secure token of claim 1, wherein processing power of the secure token is significantly less than processing power of the insecure device.

11. An article for a secure device, the secure device including a processor, the secure device used in combination with an insecure device, the article comprising memory encoded with data for instructing the processor to protect a first cryptographic key against unauthorized access, use a hash function to create a second cryptographic key from the first key and a message unique to the insecure device, and send the second key to the insecure device.

12. The article of claim 11, wherein data further instructs the processor to perform an electronic transaction to obtain the first key.

13. The article of claim 12, wherein the secure device conducts a transaction with a server to purchase a desired file; and wherein the secure device receives the first key from the server.

14. The article of claim 13, wherein the secure device conducts a transaction with a peer to purchase a file; and wherein the secure device receives the first key from the peer.

15. The article of claim 13, wherein the secure device conducts a transaction with a peer to sell a file; and wherein the secure device sends the first key to the peer.

16. The article of claim 15, wherein the data further instructs the processor to create a third key that is unique to the peer, sends the third key to the insecure device and the peer.

17. A data rights management server for use with a media transaction system, the server comprising a processing unit programmed to cause the server to establish a secure channel with a smart card, access a unique identifier corresponding to an insecure device, send a first cryptographic key to the smart card via the secure channel, receive a unique identifier from the insecure device, create a second key from the first key and the identifier, encrypt a media file with the second key, and send the encrypted media file to the insecure device, the first key corresponding to the media file.

18. The server of claim 17, wherein the smart card and the server perform an electronic transaction for the first key.

19. A method of using an insecure decryption device for file distribution, the method comprising:

accessing a message unique to the insecure device;

accessing a first cryptographic key;

creating a second cryptographic key from the message and the first key; and

allowing the insecure device to access the second key but not the first key; whereby the insecure device can use the second key for decryption.

20. The method of claim 19, wherein a hash function is used to create the second key from the message and the first key.

21. The method of claim 19, wherein accessing the first key includes performing an electronic transaction to obtain the first key.

22. The method of claim 21, wherein the electronic transaction is conducted with a server to purchase a desired file; and accessing the first key includes receiving the first key from the server.

23. The method of claim 21, wherein the electronic transaction is conducted with a peer to purchase a file; and wherein accessing the first key includes receiving the first key from the peer.

24. The method of claim 21, wherein the electronic transaction is conducted with a peer to sell a file; the method further comprising sending the first key to the peer.

25. The method of claim 24, further comprising creating a third key that is unique to the peer, and sending the third key to the insecure device and the peer.

26. An insecure decryption device for use with a secure device and a first cryptographic key, the device comprising:

means for sending a message to the secure device, the message unique to the insecure device;

means for receiving a second cryptographic key from the secure device, the second cryptographic key derived from the message and the first cryptographic key; and

means for performing decryption with the second cryptographic key.

27. The device of claim 26, further comprising means for playing media decrypted with the second cryptographic key.

28. A trusted system for file distribution, the system comprising:

an insecure device; and

a trusted secure device for storing a first cryptographic key, accessing a message from the insecure device wherein the message is unique to the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting file access rights;

the insecure device not allowed to access the first key, the insecure device using the second key for decryption.

29. (Canceled).

30. The system of claim 28, wherein the secure device is a secure token.

31. The system of claim 30, wherein the secure token includes a smart card.

32. The system of claim 31, wherein the insecure device includes a media player.

33. The system of claim 28, wherein the secure device is configured to perform an electronic transaction to obtain the first key.

34. The system of claim 28, wherein processing power of the secure device is significantly less than processing power of the insecure device.

35. The system of claim 28, further comprising a peer-to-peer application for identifying peers having desired files.

36. A trusted media transaction system comprising

an insecure media player; and

a trusted secure token for performing an electronic transaction to obtain a first cryptographic key, accessing a message from the insecure device wherein the message is unique to the insecure device, creating a second cryptographic key from the message and the first key, and allowing the insecure device to access the second key, the first key granting media file access rights;

the insecure device configured to use the second key for media file decryption.

(10) Evidence Appendix

Attached is a copy of Kocher et al., "The SSL Protocol Version 3.0", November 18, 1996, which is relied on by the Examiner to interpret the teachings of Aziz for the rejection of claims 1-3, 4 and 11-13 under 35 U.S.C. §102(e) as being anticipated by Aziz.

PATENT

Atty Docket No.: 200207237-1
App. Ser. No.: 10/733,434

(11) Related Proceedings Appendix

None.